The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/23/2009
11/24/2009 - **UPDATED**

SUBJECT:
Vulnerability in Microsoft Internet Explorer Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. **At this point in time, no patches are available for this vulnerability.** Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may cause denial-of-service conditions.

Please note: Exploit code has been published and is publically available.

November 24 - UPDATED OVERVIEW:
Microsoft has issued an advisory (see updated references below) and is investigating this vulnerability.

SYSTEMS AFFECTED:

Microsoft Internet Explorer 6.0
Microsoft Internet Explorer 7.0

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

ORIGINAL DESCRIPTION:
A vulnerability has been identified in Microsoft Internet Explorer that could allow remote code execution which is caused by a buffer-overflow condition due to a malformed record value. This vulnerability can be triggered by opening a specially crafted web page or by clicking on a link in an email. The vulnerability is related to the handling of the 'Style' HTML tag when accessed via the 'document.getElementsByTagName' Javascript function. The vulnerability allows the attacker to corrupt memory and influence a dangling function pointer in the Microsoft HTML viewer.

Successful exploitation could allow an attacker to execute arbitrary code on the affected system. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Failed exploitation could result in denial-of-service conditions.

Please note: Exploit code has been published and is publically available. We have confirmed in our lab that the current exploit code causes a denial of service condition.

ORIGINAL RECOMMENDATIONS:
The following actions should be taken:

- Consider disabling Active Scripting until a vendor patch is applied.
- Consider upgrading to Microsoft Internet Explorer 8.
- If your organization has deployed alternate browsers, recommend staff utilize an alternate browser not currently vulnerable to this attack.
- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- If you believe you have been affected by targeted attacks exploiting this vulnerability, please follow your organization's policies for incident reporting.

November 24 - UPDATED RECOMMENDATIONS:

Enable DEP for Microsoft Internet Explorer (Microsoft KB Article 977981: http://support.microsoft.com/kb/977981)

ORIGINAL REFERENCES:
Security Focus:
http://www.securityfocus.com/bid/37085

SANS:
http://isc.sans.org/diary.html?storyid=7624

Vupen:
http://www.vupen.com/english/advisories/2009/3301

Secunia:
http://secunia.com/advisories/37448/

Computerworld:
http://www.computerworld.com/s/article/9141278/New_attack_fells_Internet_Explorer

November 24 - UPDATED REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/advisory/977981.mspx
http://support.microsoft.com/kb/977981

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3762